(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－239828

(43)公開日　平成７年(1995)９月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI	技術表示箇所
G06F	15/00	330 A	7459－5L		
	9/06	550 B	7230－5B		
G09C	1/00		9364－5L		
H04H	1/02	E			
				H04L 9/02 Z	

審査請求　未請求　請求項の数12　ＦＤ　（全 7 頁）　最終頁に続く

(21)出願番号　特願平7－30268

(22)出願日　平成７年(1995)１月27日

(31)優先権主張番号　１８７５８０

(32)優先日　1994年１月27日

(33)優先権主張国　米国（US）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　アブヒジット　ケー．チョドゥリ
アメリカ合衆国，07076　ニュージャージー，スコッチ　プレインズ，アプト．ジー，パーク　アベニュー　519

(74)代理人　弁理士　三俣　弘文

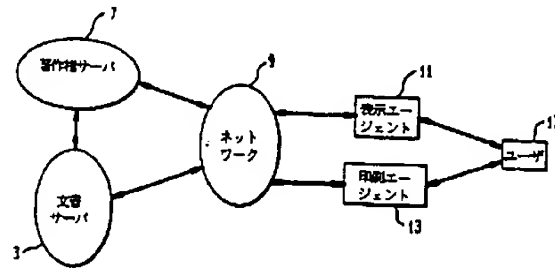
最終頁に続く

(54)【発明の名称】　電子出版文書を保護する方法

(57)【要約】

【目的】　電子出版において、不正コピーを防止し原ユーザの追跡を向上させる。

【構成】　まず、表示装置またはプリンタのあるコンピュータを有する複数のユーザから、文書に対する要求を固有のユーザ識別情報とともに受信する。次に、複数のユーザからの要求を著作権サーバで認証する。次に、著作権サーバは、文書サーバに対し各要求の正しい認証に作用するよう指令する。これに応答して、文書サーバは、認証された各要求に対して、独自に符号化され圧縮され暗号化された文書を作成し、認証された各要求ユーザへの文書を、ネットワークを通じて、認証された各要求ユーザの対応する表示または印刷のエージェントへ転送する。文書は、複数のユーザのそれぞれに対応して独自に符号化される。最後に、各エージェントで文書の復号および圧縮解除を行い、認証された要求ユーザによってエージェントに提供された正しい秘密鍵にのみ応答して文書を利用可能にする。



【特許請求の範囲】

【請求項１】　文書の電子出版のためにコンピュータシステムおよびネットワークを動作させる際に電子出版文書を保護する方法において、
前記ネットワークによって前記コンピュータシステムに接続されたコンピュータを表示装置またはプリンタとともに有する複数のユーザから、各ユーザに固有のユーザ識別子を含む文書要求を受信するステップと、
前記要求を著作権サーバで認証するステップと、
前記著作権サーバが、文書サーバに対して、認証された各要求に作用するよう指示するステップと、
前記著作権サーバからの前記指示に応答して、前記文書サーバが、各認証された要求に固有の識別子とともに暗号化された文書を作成し、その文書を前記ネットワークを通じて各認証された要求したユーザの、表示エージェントおよび印刷エージェントから選択される対応するエージェントへ転送するステップと、
作成した各文書が前記固有の識別子に基づいて固有に符号化されるように前記文書を符号化するステップと、
認証された要求したユーザによって提供された正しい秘密鍵が前記エージェントで受信されたことにのみ応答して、前記エージェントにおいて前記文書を復号し、前記文書を利用可能にするステップとからなることを特徴とする、電子出版文書を保護する方法。

【請求項２】　前記文書サーバは前記文書を圧縮し、前記エージェントは、前記認証された要求したユーザによって提供された正しい秘密鍵を受信したことに応答して、前記文書を圧縮解除することを特徴とする請求項１の方法。

【請求項３】　前記エージェントは各ユーザのコンピュータにソフトウェアとして事前にインストールされていることを特徴とする請求項１または２の方法。

【請求項４】　前記エージェントは要求の認証後にのみ前記複数のユーザに伝送されるソフトウェアプログラムであることを特徴とする請求項１または２の方法。

【請求項５】　前記エージェントは、表示装置およびプリンタから選択されるユーザハードウェア内に、ハードウェアおよびファームウェアから選択されるコンピュータウェアとして事前にインストールされていることを特徴とする請求項１または２の方法。

【請求項６】　前記エージェントはユーザに対応して固有の内部コードを有することを特徴とする請求項１または２の方法。

【請求項７】　前記エージェントは、出版文書の単一の固有に符号化されたバージョンのみを復号することが可能であることを特徴とする請求項１、２、３またはうの方法。

【請求項８】　前記複数のユーザは、固有の正しいユーザ秘密鍵に応答して復号および表示をするためにシステム識別子から鍵を導出するアルゴリズムを使用する同一のエージェントを有することを特徴とする請求項１の方法。

【請求項９】　前記複数のユーザは、転送された各文書とともにエージェントを受信し、それらすべてのエージェントは与えられた文書に対しては同一であるが出版ごとに異なることを特徴とする請求項１の方法。

【請求項１０】　前記複数のユーザは、転送された各文書とともにエージェントを受信し、それらすべてのエージェントは相異なることを特徴とする請求項１の方法。

【請求項１１】　前記文書は前記文書サーバによって固有に符号化されることを特徴とする請求項１または２の方法。

【請求項１２】　前記文書は、各認証された要求したユーザに転送された後に固有に符号化されることを特徴とする請求項１または２の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号プロトコルを使用して電子出版物を保護する方法に関する。本発明は、ソフトウェアまたはハードウェアの特別の「エージェント」を利用して、表示装置（ディスプレイ）やプリンタに対し、文書の復号をしてからその表示または印刷を行うように要求する。本発明の方法は、電子出版文書の不正な再版またはコピーを阻止する。

【０００２】

【従来の技術】暗号および識別確認は、従来、ネットワークを通じてのコンピュータ伝送とともに記述されている。例えば、米国特許第４，３９３，２６９号には、トランザクションおよび識別確認に対する一方向シーケンスを組み込む方法が記載されており、米国特許第４，９９５，０８２号には、データ交換方式において、加入者（購読者）を識別し、電子署名を生成し確認する方法が記載されている。米国特許第５，１４４，６６５号には、暗号通信の方法およびシステムが記載されている。

【０００３】

【発明が解決しようとする課題】これらの米国特許は暗号技術ならびに鍵の識別およびアクセスの方法を使用しているが、いずれにも、本願発明のシステムのように、不正コピーを防止し、原ユーザの追跡を向上させた技術の組合せは記載も示唆もされていない。

【０００４】

【課題を解決するための手段】本発明は、電子出版文書を保護する方法に関する。本発明は、文書の電子出版のためにコンピュータシステムおよびネットワークを動作させる方法に係るものであり、以下の（ａ）～（ｅ）のステップからなる。

【０００５】（ａ）表示装置またはプリンタのあるコンピュータを有する複数のユーザから、文書に対する要求を受信するステップ。この要求とともに、複数のユーザのそれぞれの固有のユーザ識別情報を要求する。

【０００６】（ｂ）複数のユーザからの要求を、著作権サーバで認証するステップ。
【０００７】（ｃ）著作権サーバを使用して、文書サーバに対し、各要求の正しい認証に作用するよう指令するステップ。
【０００８】（ｄ）著作権サーバからの指令に応答して、文書サーバを使用して、認証された各要求に対して、独自に符号化され圧縮され暗号化された文書を作成し、認証された各要求ユーザへの文書を、ネットワークを通じて、認証された各要求ユーザの対応するエージェントへ転送するステップ。文書は、複数のユーザのそれぞれに対応して独自に符号化され、各エージェントは、ディスプレイエージェントおよびプリンタエージェントから選択される。
【０００９】（ｅ）各エージェントにおいて文書の復号および圧縮解除を行い、認証された要求ユーザによってエージェントに提供された正しい秘密鍵の受信にのみ応答して文書を利用可能にするステップ。
【００１０】これらのエージェントは、複数のユーザのそれぞれのコンピュータにプレインストールされるか、表示装置およびプリンタから選択されるユーザハードウェア内にハードウェアまたはファームウェアとしてプレインストールされるか、または、使用時に伝送されるソフトウェアプログラムであるかのいずれかである。
【００１１】
【実施例】
［１．はじめに］ファクシミリの利用の増加により、紙文書の電子転送が受け入れられるようになってきた。電子メール、電子掲示板および大規模ネットワークシステムにより、電子情報を大きいグループに配布することが可能である。さらに、パーソナルコンピュータおよびワークステーションの普及、優れた品質のデスクトッププリンタ、および、大量の電子データ用の記憶装置の価格の急落により、文書を電子的に表示し、印刷し、記憶することが技術的に実現可能になった。これらのすべての発展は、電子出版を現実のものにした。情報の電子配布は、紙のコピーを作成してそれを輸送するよりも高速であり、安価であり、必要な労力が少ない。電子情報配布に有利な他のファクタには、コンピュータを使用して特定の情報を検索する能力、および、受容者に配布されるものを容易にカスタマイズする能力がある。電子的な新聞、雑誌および機関誌は、現在の紙配布ネットワークを補完し、最終的には置き換わる態勢ができている。
【００１２】電子配布によって与えられる効果は、紙バージョンに置き換わるものとしての電子文書の受容に対する主な技術的障害のうちにもある。電子出版が直面する主要な技術的かつ経済的困難のうちの１つは、個人が電子文書を容易にコピーし不法に配布することのないようにすることである。電子文書を受け取った人は、それを大きいグループに転送することは、同じ文書の紙のコピーを受け取った人よりも容易である。さらに、電子コピーは、紙のコピーよりも原物に似ている。電子コピーが作成されると、原物の所有者および受容者は同一物を有することになる。電子文書の違法コピーは、収入の多大な損失を引き起こしかねない。
【００１３】そこで、本発明は、暗号プロトコルを使用して、利用可能な配布および表示の技術によって（代表的には、プリンタおよび表示装置を使用して）不正な電子コピーの配布をすることを思いとどまらせ、または、防止することに関する。ここで使用する「プリンタ」という用語は、機械的またはレーザ方式のプリンタ、ファクシミリ機、複写機、プロッタなどを含むように広義に解釈されることを意図している。同様に、「表示装置」は、印刷形式以外の任意の形式で文書を表示する任意の装置を含むように広義に解釈されるべきである。本発明は、電子文書配布を安全にするための２つの方法を提供する。いずれの場合にも、出版者は秘密鍵で文書を暗号化する。第１の方法（第３．１節）では、プリンタまたは表示装置内の専用のハードウェアまたはハードウェアが文書を復号する。そのユーザのみが文書の暗号化バージョンにアクセスすることができるのみで、他人は使用できない。
【００１４】第２の方法（第３．２節）では、文書は受容者のコンピュータ内のソフトウェアによって復号される。専用のハードウェアまたはファームウェアは必要でないが、ビットマップがユーザに利用可能であり、配布可能である。この方法では、出版者は文書を暗号化し、周知のポストスクリプト言語のようなページ記述言語（以下「ＰＤＬ」という。）でその文書を伝送し、復号プログラムがビットマップを生成する。出版者は、文書のＰＤＬバージョンにおいて、容易に行間または単語間の間隔を変更して、文書の各コピーを固有のものとすることができる。この方法には、違法コピーの配布を思いとどまらせる２つの要素がある。
【００１５】１．著作権法に違反する違法コピーは原物所有者までさかのぼって追跡可能である。
２．ビットマップ、またはそのビットマップの簡易圧縮バージョンは、ＰＤＬバージョンよりビット数が多いため、違法配布者は出版者よりもその文書を伝送するのにコストがかかる。
【００１６】この方法はまた、出版者にとって、固有の文書識別のための伝送コストが減少する。固有の識別子は、ＰＤＬバージョンからは容易に削除されるが、ビットマップからは容易には削除されない。暗号化によって、出版者は、ユーザのアクセスを可能にすることなく、ＰＤＬバージョンを伝送することができる。
【００１７】復号を実行可能なプロセッサのコストはプリンタおよびディスプレイのコストに比べて高くない。従って、電子出版が広まってしまえばおそらく第１の方法が使用されるだろうと予想されるかもしれない。しか

し、電子出版が広範に使用されるまでは、内部復号機能を有する出力装置が存在する可能性は少ない。第２の方法は、専用ハードウェアが広く受け入れられる前に本発明の目的を達成する受容可能な手段を提供するものである。第２の方法は違法コピーを思いとどまらせるだけでそれを阻止するものではないが、より広いクラスの電子出版を可能にするものである。適当な数の電子出版が利用可能になれば、専用ハードウェアも普及するであろう。

【００１８】［２．アーキテクチャ］本発明による電子文書の配布の基本的アーキテクチャを図１に示す。ここで、文書サーバ３（出版者により信頼されている）は、符号化、暗号化および圧縮された文書をユーザ１７に提供する。著作権サーバ７は、ユーザ１７からの、文書を取得しようとする要求を認証する。これも出版者によって信頼されている。表示エージェント１１は、文書サーバ３から取得した文書を復号し表示するソフトウェアを含む。このソフトウェアは出版者により信頼されている。印刷エージェント１３は、文書サーバ３から取得した文書を復号し印刷するソフトウェアを含む。このソフトウェアは出版者により信頼されている。表示エージェント１１もしくは印刷エージェント１３のいずれか、もしくはその両方、またはこれらを複数個、ユーザは利用可能である。

【００１９】ネットワーク９は、文書要求および文書を他の構成要素との間で伝送する。ユーザ１７は文書に対する署名した要求を生成し、文書の表示または印刷をするためには秘密鍵を提示する必要がある。

【００２０】［３．提案する実施例］電子文書配布を安全にするための２つの一般に別個の実施例を提案する。第１の方法は、電子文書を表示または印刷するために専用ハードウェアを必要とし、このような専用装置が安価で容易に利用可能であるような段階にハードウェア技術が進歩したときにはより適当である。第２の方法は現在利用可能な表示装置およびプリンタを利用する。しかし、いずれのプロトコルも、同じ上記の基本アーキテクチャおよび方法を使用する。

【００２１】［３．１　例1］この第１の実施例（図２）は、文書サーバ１０３（出版者により信頼されている）と、信頼された表示エージェント１１１または信頼された印刷エージェント１１３との間で暗号化された情報を送信する暗号技術の直接的応用である。表示エージェント１１１または印刷エージェント１１３は、著作権サーバ１０７と共有する秘密鍵を含み、電子出版用に設計された専用の表示装置１２１またはプリンタ１２３内にある。ここで、エージェントとは、指定された入力にのみ応答して復号を行う、必要なソフトウェア、ハードウェア、またはファームウェアを意味する。これらの装置は、秘密鍵を含むハードウェアまたはファームウェアのコピーが容易にできないように密封されなければならない。

【００２２】ユーザ１１７が文書の閲覧または印刷をしたいときには、ネットワーク１０９を通じて、固有の識別を使用することによって文書に対する要求をしなければならない。この固有の識別は、ユーザが他人に不正目的で教えたがらないような、クレジットカード番号などの比較的貴重な番号である。著作権サーバ１０７がユーザの要求を認証した後、文書サーバ１０３は、ユーザ空間１１５にとって利用可能な表示装置１２１またはプリンタ１２３へ直接に暗号化したコピーを送信する。この文書は、特定のプリンタまたは表示装置しかそれを復号することができないように暗号化されている。ネットワーク上では暗号化された文書しか見えないため、悪意ユーザがその文書を理解することはできない。ディスプレイまたはプリンタは、暗号化された文書を受信すると、それを復号し、表示または印刷をする。本発明の実施例によっては、もう１つの特徴として、ユーザは、表示または印刷の機能を起動するために、表示エージェントまたは印刷エージェントに、最初の要求をするために使用した固有識別番号を入力するよう要求されることも可能である。このような実施例では、不正コピーの配布を防止することができる。情報を暗号化するためにこの方法で使用されるアルゴリズムは、ＤＥＳ（公知の私的鍵方式であるディジタル暗号標準）のような標準的なアルゴリズムでよい。しかし、この実施例の方法は電子出版のための専用のディスプレイおよびプリンタを必要とするため、このような専用ハードウェアが妥当になるほど十分な数のサービスおよびユーザが存在するようになったときにはより適切になる。このようなハードウェアは従来技術の範囲内にあるが、電子出版が広く行われるまでは、少数のユーザに基づく販売が商業的に成功することは困難であろう。

【００２３】［３．２　例2］この第２の方法では、専用ハードウェアを必要としない暗号技術が使用される。通常のディスプレイおよびプリンタを扱う際に遭遇する問題は、表示または印刷される情報が受容者のコンピュータに存在するということである。受容者は、表示される情報を捕捉することができ、また、その情報を好きなだけ多くの他のプリンタおよびディスプレイに配布することができる。本発明の目的は、受容者が情報の再配布をするのを防止しようとする代わりに、違法コピーの配布を思いとどまらせることである。

【００２４】以前の研究で、各受容者用に雑誌の注文コピーをカスタマイズすることができることは、文書の原所有者を識別するために使用することも可能であることがわかっている。原所有者を識別する情報は、テキストの行間および単語間の間隔に、または、単語、行および文字の特徴における固有のシフトもしくは変化の一部として、符号化される。このメカニズムの目的は、著作権法に違反して雑誌を配布することを思いとどまらせるこ

とである。

【００２５】これから、プロトコルについて説明する。このプロトコルにより、文書は購読者に電子的に配布されることが可能となり、購読者はその文書を電子的に非購読者に配布することを思いとどまらせられる。情報を暗号化するために使用するアルゴリズムは、ＲＳＡ（周知の公開鍵方式のアルゴリズム）のような標準的なアルゴリズムでよい。本発明は、電子文書の不法な配布を思いとどまらせるための、暗号技術の新しい応用に関するものである。本実施例は、専用ハードウェアを必要としないが、本実施例の技術は、電子文書配布の実現可能性を実証し、この分野での新しいサービスを促進するのに有用であると考えられる。十分な数のユーザが存在するようになれば、専用ハードウェアは正当化され、例１のようなさらに簡単な方法が商業的観点からもうまく使用されることになろう。

【００２６】［３．２．１　プロトコルの概観］プロトコルについて、図３および以下の用語によって説明する。

【００２７】１．要求発生。ユーザｕは、ネットワーク２０９を通じて著作権サーバ２０７に対して、文書詳細を含む署名付きメッセージを送ることによって文書を要求する。

【００２８】２．文書伝送。（ａ）著作権サーバ２０７は要求を確認し、それが有効である場合、文書サーバ２０３から文書を送るよう手配する。（ｂ）文書サーバ２０３は、暗号化され圧縮されたＰＤＬバージョンの文書をユーザ２１７に送る。ユーザｕに送られる文書は、ｕに固有なある情報で符号化すなわちフィンガプリントされる。（あるいは、文書のこの符号化すなわちフィンガプリントは、ユーザ端で、例えば、ユーザのプリンタまたは表示装置によって実行されることも可能である。）また、著作権サーバ２０７は、この段階で、表示エージェント２１１および印刷エージェント２１３をユーザ空間２１５に送る。

【００２９】３．文書の閲覧または印刷。文書を表示（または印刷）する要求を受け取ると、表示エージェント２１１または印刷エージェント２１３は、ユーザ２１７に、自分の秘密鍵S_uをタイプするよう促す。エージェントはそれを受け取ると、受信したＰＤＬ文書を復号し圧縮解除して、ビットマップを生成し、それを表示装置２２１またはプリンタ２２３へ送る。

【００３０】［プロトコルの詳細］以後、ｄ、ｃ、およびｕでそれぞれ文書サーバ、著作権サーバおよびユーザを表す。各ユーザｕは公開鍵P_uと秘密鍵S_uの対を有すると仮定する。さらに、文書サーバまたは著作権サーバは、送信する文書を暗号化するために使用する鍵M_xを有する。この鍵は、表示エージェントおよび印刷エージェントが受信した文書を復号することができるように、これらのエージェント内に埋め込まれる。

【００３１】［要求発生］

m_1（ｕ，ｃ）＝［ｕ，文書情報，ES_u［ｕ，文書情報］］

これは、ユーザｕから著作権サーバｃへの、文書を要求する署名付きメッセージm_1である。文書情報（例えば雑誌、記事の題名、著者など）もユーザＩＤ（ｕ）とともに送られる。ユーザＩＤ（ｕ）を用いて著作権サーバは辞書を調べ、ユーザの公開鍵P_uを見つける。さらに、ユーザは、平文に自分の秘密鍵S_uで署名する。S_uでの暗号化Ｅは、悪意のユーザが他人になりすますのを防ぎ、文書要求の不正変更を防ぐために必要である。

【００３２】［文書伝送］著作権サーバはm_1（ｕ，ｃ）を受け取り、辞書でP_uを調べ、ES_u［ｕ，［文書情報］］を復号し、復号したテキストと平文を比較する。これらが同一である場合、文書m_3（ｄ，ｕ）をユーザに送るために、文書サーバへメッセージm_3を送る。また、この段階で著作権サーバは、表示エージェントおよび印刷エージェントをユーザに送る。表示エージェントおよび印刷エージェントには、内部に鍵Φが埋め込まれている。この鍵はEP_u［M_x］、すなわち、ユーザの公開鍵P_uで暗号化された鍵M_xである。

m_2（ｃ，ｕ）＝［［表示エージェント］，［印刷エージェント］］

m_3（ｄ，ｕ）＝EM_x［［圧縮文書］］

【００３３】特定のユーザｕ以外は、これらのエージェントを使用して、暗号化された文書を復号することはできないため、表示エージェントおよび印刷エージェントは暗号化されない。

【００３４】ユーザに送られる文書は、M_xで暗号化された、圧縮ＰＤＬバージョンである。文書を暗号化するのに用いた鍵M_xはS_uなしにはΦから生成することができないため、ユーザｕが暗号化された文書とともに表示エージェントまたは印刷エージェントを配布したとしても、秘密鍵S_uが知られない限りはそのエージェントは役に立たない。

【００３５】［文書の閲覧または印刷］文書を閲覧（または印刷）するために、表示（印刷）エージェントはまずユーザに秘密鍵S_uの入力を促す。埋め込まれた鍵ΦがS_uで復号され、鍵M_xを取得し、これを用いて圧縮された文書が復号される。これはさらに圧縮解除され、ビットマップに変換されて、画面（プリンタ）に送られる。

【００３６】上記のプロトコルによって、正当なユーザは、必要な回数だけ、文書を要求しそれを自分の端末またはワークステーションで閲覧することができる。しかし、違法なユーザは、たとえ表示（印刷）エージェントをおよび暗号化された文書を正当ユーザからコピーしたとしても、同じことはできない。プロトコルの基礎となっている仮定は、ユーザの秘密鍵S_uはユーザにとって非常に重要であるため公開することができないようなも

のであるということである。秘密鍵が、電子メール署名、システムログインまたはクレジットカードによる購入に使用されるものと同一である場合、それを他人にもらすことには強い抑制が働く。

【００３７】また、文書が表示または印刷されるのを、事前に登録されたハードウェアに何らかの方法で制限することによって、さらに予防措置を組み込むことができる。しかしこれはユーザを特定のマシンに結びつけユーザの可動性を制限するので好ましいことではない。

【００３８】文書は、復号され圧縮解除されると、ユーザのコンピュータでビットマップとして利用可能である。ここで想起すべき点であるが、（１）ビットマップはユーザｕに固有の情報でフィンガプリントされており、（２）ビットマップは出版者によって伝送された圧縮ＰＤＬバージョンの文書よりもずっと大きい。従って、たとえユーザがそのずっと大きいビットマップファイルを捕捉し伝送しようとしても、そのユーザは、ビットマップからフィンガプリントを消去するのに多大な労力をつぎ込まない限り、自分を罪に陥れる危険を冒してしかそのようなことはできない。

【００３９】［３．２．２　鍵隠蔽メカニズムとしての一回使用プログラム］例２で指摘したように、文書を表示し印刷するためには、ユーザの制御下で、重要なプログラムが実行される必要がある。例えば、表示エージェントまたは印刷エージェントがある。これは、内部に出版者の魔法の鍵M_xが隠蔽された、信頼されたプログラムである。実行中に、表示（印刷）エージェントはしかるべき場所から$ES_u[M_x]$を取り出し、ユーザｕによって提供されたS_uを使用してそれを復号し、それを使用して、暗号化された文書を復号する。注意すべき点であるが、表示（印刷）エージェントのコードを解析し、しかるべき点で実行を停止することによってユーザがM_xを発見することができる場合、暗号化された文書を送信する全体の目的は破れる。この種のリバースエンジニアリングを完全に防止することはできないため、同じ仕事をするが各ユーザには異なって見える信頼されたプログラムを送ることによってリバースエンジニアリングの利益を縮小している。文書および表示（印刷）エージェントをネットワークを通じて配布する場合、各受容者に固有のコピーを生成することは比較的容易である。

【００４０】一回使用プログラムを使用することは、プログラムの原本を容易に追跡することができるという利点も有する。バイナリ実行可能プログラムを変更して他の動作するプログラムを作成することは、プログラム構造およびプログラムが使用している自己保護メカニズム（チェックサム）の深い理解を必要とする。印刷された記事を保護することに比べて、プログラムを識別することは比較的容易である。

【００４１】例えば、以下のように、機密性（セキュリティ）の４つの異なるレベルが使用される。

【００４２】１．システム識別子から鍵を導出するアルゴリズムを含む同一の表示（印刷）エージェントをすべてのユーザが有する。

【００４３】２．表示（印刷）エージェントを１度（または、各ユーザに固有のある時間間隔で）送る。

【００４４】３．表示（印刷）エージェントは各文書に対して同一であり、各文書とともに伝送される。

【００４５】４．表示（印刷）エージェントは別個であり、各文書とともに伝送される。

【００４６】コンパイルまたはリンク段階で自動的に、別個であるが同等のプログラムを作成するためにはいくつかの技術が使用可能である。例えば、

（１）リンカはテキストおよびデータセグメントを再配置することができる。

（２）コンパイラに、あるコードのセクションをランダムに最適化するように命令することができる。

（３）コードのセクションは機能的に同等の異なるアルゴリズムで置換可能である。

（４）コンパイラはレジスタ割当て順序を変更することができる。

【００４７】ＲＡＭアクセスパターンおよび内容を保護するために、実行効率が低下するという犠牲を払って、さらに入念な方法を追加することも可能である。さらに、点検コードシーケンス（例えば、定数アドレスへのシステムコールを計算されるコールで置換する）を隠蔽する標準的方法も使用可能である。

【００４８】

【発明の効果】以上述べたごとく、本発明によれば、電子出版において、不正コピーを防止することができる。

【図面の簡単な説明】

【図１】電子出版物を保護する本発明の方法の全体のアーキテクチャの図である。

【図２】専用ハードウェアを使用した、本発明の方法の特定のアーキテクチャの図である。

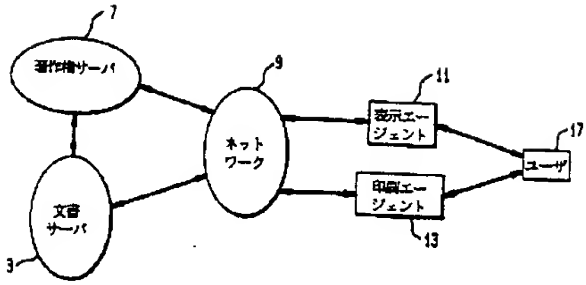
【図３】専用ソフトウェアを使用した、本発明の方法の特定のアーキテクチャの図である。

【符号の説明】

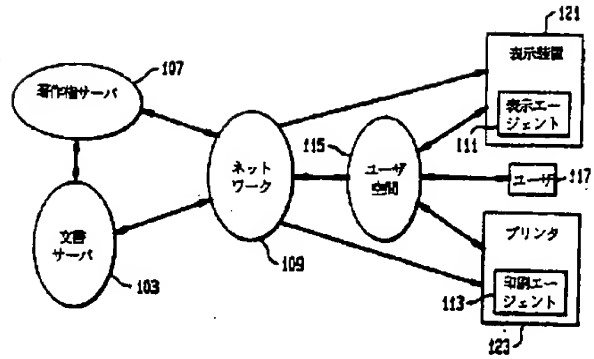
３　文書サーバ
７　著作権サーバ
９　ネットワーク
１１　表示エージェント
１３　印刷エージェント
１７　ユーザ
１０３　文書サーバ
１０７　著作権サーバ
１０９　ネットワーク
１１１　表示エージェント
１１３　印刷エージェント
１１５　ユーザ空間
１１７　ユーザ

１２１　表示装置
１２３　プリンタ
２０３　文書サーバ
２０７　著作権サーバ
２０９　ネットワーク
２１１　表示エージェント
２１３　印刷エージェント
２１５　ユーザ空間
２１７　ユーザ
２２１　表示装置
２２３　プリンタ

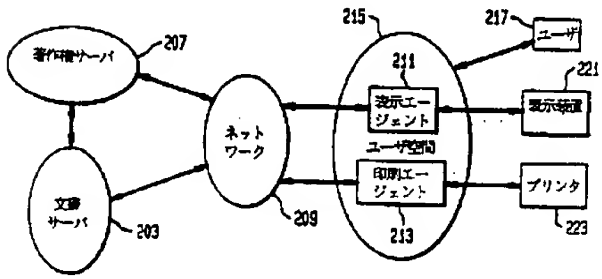
【図１】



【図２】



【図３】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｈ　1/08				
Ｈ０４Ｌ　9/06				
9/14				

(72)発明者　ニコラス　エフ．マクセムチュク
アメリカ合衆国、07092　ニュージャージー、マウンテンサイド、ローリング　ロック　ロード　355

(72)発明者　サンジョイ　ポール
アメリカ合衆国、07076　ニュージャージー、スコッチ　プレインズ、カントリー　クラブ　レーン　219

(72)発明者　ヘニング　ジー．シュルツリネ
アメリカ合衆国、07980　ニュージャージー、スターリング、アプト．８、サマセット　ストリート　324